LAUREA
UNIVERSITY OF APPLIED SCIENCES
Together we are stronger

Employer's legal duty of care and security risk management in high-risk environments: a theory-based case study of the gross negligence of Norwegian Refugee Council in 2015

Johannes Laaksonen

2018 Laurea

Laurea University of Applied Sciences

Employer's legal duty of care and security risk management in high-risk environments: a theory-based case study of the gross negligence of Norwegian Refugee Council in 2015

Johannes Laaksonen
Degree Programme in Security Management
Bachelor's Thesis
May, 2018

Laurea University of Applied Sciences **Abstract**
Degree Programme in Security Management
Degree programme in Security Management

Johannes Laaksonen

Employer's legal duty of care and security risk management in high-risk environments: a theory-based case study of the gross negligence of Norwegian Refugee Council in 2015

2018 Pages 50

This thesis is a study of the Oslo District Court 2015 ruling of gross negligence on the part of the Norwegian Refugee Council (NRC) towards its staff consultant Patrick Dennis. Mr. Dennis was on an assignment in Kenya in 2012, when his convoy was attacked. He was shot in the leg, kidnapped and held for a period of time before rescue. He later sued NRC for damages sustained, and won in court.

The court case was a first for the industry, a landmark case of a humanitarian organization found guilty of a serious breach of duty of care. It has prompted humanitarian organizations to paying increasingly careful attention to their practices of managing security in their challenging high-risk operational environments.

This thesis is a case study of the failures by the NRC to properly establish reasonable security risk management practices. Commissioned by the Finnish NGO Crisis Management Initiative, it also attempted to draw lessons learned for the industry in managing their security in a more effective manner. The study is a theory-based content analysis that compares the theoretical and knowledge framework of the ISO31000:2009 risk management model to the official Oslo District Court ruling of 2015. The Oslo District Court ruling does not refer to risk management directly. In analysing the ruling, the study used the methodologies of theory-based content analysis in finding implicit parallels and meanings in the ruling that can be compared with the different steps of the risk management model. It attempted to find meanings in the text of the ruling that referred to failures in establishing the risk management context, in risk identification, in risk assessment and in risk treatment.

They key finding was that the Oslo District Court ruling can be interpreted to have implicitly referred to failures for NRC during all steps of the risk management model used as the theoretical base. Failures were many and are listed in detail in the findings. Furthermore, for the security management model proposed in this thesis to be effective, the NRC ruling showed that absolute care must be placed to conduct the risk management process properly from the beginning. NRC's failures were, to a large extent, failures made when the risk management process was begun.

Furthermore, all the findings are summarized in a table that is used by the commissioning organization and other interested parties as a reference on how, if applying the ISO31000:2009 model, similar incidents can be avoided in the risk management practices in the future.

Keywords: risk management, ISO31000:2009, duty of care, humanitarian aid, gross negligence

Table of Contents

1 Introduction

Humanitarian aid organizations can be seen as a fringe element in the bigger picture of businesses and organizations that operate globally and across borders. They rarely work for-profit, and often have full-time staff working in high-risk environments. They can receive spectacular media attention during times of humanitarian crises, but number only a fragment of total organizations with regular cross-border operations. A specialist field, the demands of their high-risk operational environments place exceptional requirements for their security and safety risk management structures. While for the larger for-profit enterprises and government organizations, a structured security management requirements and rigorous audits can often be a regular experience, aid organizations often rely on the vague concept of acceptance for ensuring the security and safety of their staff members (Humanitarian Practice Network, 2010). Who would attack our organization if we are neutral and only there to protect innocent civilians suffering from the crisis?

Humanitarian organizations, however, face numerous major attacks to their staff members each year. Furthermore, the total number of incidents is vastly increased if safety related incidents are included in the statistics. (Humanitarian Outcomes, 2017, 1). The nature of the humanitarian work is to operate where their help is needed the most. While this remains, in my opinion, truer than ever, and the number of humanitarian crises remains high, the operational realities must be balanced with the fact the many armed actors and conflict parties often see international, especially Western-led, non-governmental aid organizations (INGOs) as non-neutral extensions of the diplomacy practiced by their donor governments (Humanitarian Policy Group, 2012, 10). This can make the aid organization a tempting target for political violence. The risk of operating in these vulnerable environments is further amplified by looking at common robberies, abuse, safety incidents, medical risk in unsanitary conditions and psychological pressure. It can be said that aid workers put their life and health on the line every time they get off the plane and go to work. In my opinion, aid workers also tend to be idealistic people who accept a high amount of personal risk for the greater good of the results of their work. This is evident in the research where aid workers in the field were surveyed on whether their organization has become more or less risk-tolerant in recent years. 79% of the people who answered did so with a yes (Humanitarian Outcomes, 2016, 10). The high risk-appetite and the reliance on acceptance, based on my observations, also reflect the relatively relaxed attitudes that aid organizations take in terms of security and safety risk management.

Funding for humanitarian initiatives has been growing more slowly during recent years. Some major donors, such as the Gulf states, have cut their funding significantly (Development Initiatives, 2017, 44). This has become apparent with the populist and protectionist movements in the West and elsewhere. The lack in funding can result, according to my

personal observations, in increased pressure to deliver aid and still make meaningful impact while cutting from the administrative and support function costs. Security management can often be the first head on the block for organizations desperate to keep their core activities alive in an environment of dwindling funding.

With the security function scaled down, aid organizations are left with tremendous vulnerabilities. The loss of assets in the case of incidents can be difficult to recover from. The loss of human life can be a trauma to the organization that it will never fully recover from. The loss of operational capacity due to an incident can lead to increased tragedy and suffering among the local populations that the organization is trying to help. The loss of reputation and liquidity in an event of a major litigation for staff security negligence can be detrimental and act as a long-term hindrance.

European and Western aid organizations can, in my opinion, sometimes have a problematic relation to occupational health, safety and security legislation (sometimes referred to as *legal duty of care*) of their home countries. This stems from the unique nature of their working environment vis à vis the broad nature of the legislation. Usually, the related safety laws are intended for a wide spectrum of organizations, clear majority of which represent the local service and production industries. The interpretation of "reasonable and justifiable" security measures to be taken by an organization to protect its staff while in the workplace is relatively easy to transfer to regular businesses and organizations. For example, the laws for office safety and security tackle tangible questions related to ergonomics and common safety hazards around the office space. The matter is more complicated for the aid industry. How do the courts define safety and security *in the workplace,* when the workplace is, for example, a refugee camp in Mosul instead of the local supermarket in Helsinki? Do the courts make a distinction between these two, or do they mean that workplace is simply the location where your staff works? In case of a complex high-risk location, how does the employer determine if the security risk management and risk treatment measures taken were reasonable and justifiable – instead of negligent? What is the minimum of security risk management needed for these locations to fulfil the broad requirements set by the laws, and how is that minimum threshold interpreted in the case of an incident tried in court? These are just a few questions which can trouble managers in humanitarian and other organizations that operate in high risk environments, but are registered in countries such as Finland where legislation is strict on the legal duty of care of an employer.

Aid organizations had, in the past, not experienced serious litigation due to negligence in matters of staff safety and security. Most of the incidents had been quietly settled out of courts between the families and the organizations. The question of common occupational health and safety legislation, and its relation to aid organizations that routinely operate in

high-risk contexts had not been an exercise that had been tested in court and no precedent existed (Oslo District Court, 2015, 13).

This changed in November 2015. Three years earlier, in 2012, a Canadian contractor Steven Patrick Dennis was on a mission in Kenya for the Norwegian Refugee Council (NRC). NRC is an organization that supports refugees and displaced people. During a VIP visit to IFO II refugee camp in Dabaab where the executive director of the organization was present, he and his colleagues were attacked and kidnapped. Their driver was shot dead during the kidnap operation, and Dennis sustained an injury to his knee. Dennis and his remaining colleagues were released four days later in a military operation orchestrated by the local police and a detachment from the local armed militia. In February 2015, Dennis sued NRC for his economic and non-economic losses after the incident. Later that year, the Norwegian courts ruled that NRC had acted with gross negligence in relation to staff safety and security (Oslo District Court, 2015, 11). The organization had to pay substantial compensation to Dennis. The reputation risk also amounted to loss of trust with partners and donors for the NRC to operate safely and manage the security of their staff. The duty of care of NRC was found to have been vastly lacking.

More importantly, Dennis v Norwegian Refugee Council case and its ruling set the precedent for a new era in which aid organizations, and indeed *any organizations working in high-risk areas*, are as liable as any other company or organization to fulfill their duty of care towards their staff members – consultant or otherwise. The idea that humanitarian exceptionalism might protect them from litigation was gone. The idea that legal duty of care of the country where the organization is based in did not extend to contractors or foreign operations had been erased. Many parties called the case “a game changer” and “a wake-up call” for the humanitarian aid industry with regards to their policies for staff safety and security (IRIN, 2015). NRC practiced security management, had policies in place and had dedicated security advisers who worked on staff security on a daily basis – yet their approach was ruled inadequate by the Norwegian courts.

This thesis is a detailed case study on the Dennis v. Norwegian Refugee Council 2015 case from the perspective of a ISO31000:2009 based risk management model used by the commissioning organization of the thesis. It attempts to tackle the court’s ruling from the perspective of risk management, draw conclusions as to how NRC failed in their risk management during every step of the process – and finally draw lessons learned for the commissioning organization and the industry as a whole.

Even though the case is relatively recent, it has been subject to numerous news articles and analyses. At least one substantial study has been published on the incident and its implications for security risk management. A major publication called “Duty of Care: A review

of the Dennis v Norwegian Refugee Council ruling and its implications" was published by the European Inter-Agency Security Forum (EISF, 2016). It studied the court case from the perspective of drawing practical lessons learned from the incident, and how all organizations, regardless of their risk management structures, can implement measures that benefit security management and promote duty of care. The previous study focuses on "the interrelation between the ruling, Duty of Care and security risk management (EISF, 2016, 8)." This study takes a different approach, and approaches the subject from a clear ISO31000:2009 risk management perspective. In this study, the duty of care is seen as a by-product of an effective and formal risk management process. Duty of care is not approached solely as a legal term from the perspective of analysing the court's rationale for passing judgement on organization's negligence. The previous study placed more emphasis on the court's decision for a minimum legal duty of care requirements from the perspective of security management. In this study, the court case and its ruling will be analysed rigorously from the perspective of a pre-defined theoretical framework of risk management. The findings of this study will complement previous research on the topic by providing a more thorough risk management - specific perspective to the case. Industry professionals can benefit from the combined analysis of this study and the previous study complied on the topic, as both the findings of will contribute to a more thorough and complete understanding of how major incidents like this can be avoided.

Furthermore, it is important to highlight that the International Organization for Standardization (ISO) has, since February 2018, launched a revised and updated version of their risk management standard. Called ISO31000:2018, it is an updated iteration on ISO31000:2009 and places more considerable emphasis on decision-making structures and continuous improvement models of risk management (ISO, 2018). This research was undertaken when ISO31000:2009 was still the dominant framework. Regardless of the new model, this research remains relevant as the basic risk management process used as the theory-base in this study remains unchanged from ISO31000:2009 to ISO31000:2018 (International Organization for Standardization, 2018). This study will refer to the ISO31000:2009.

2 Research question

This thesis is a detailed case study on the Dennis v Norwegian Refugee Council case of 2015 from the perspective of security and safety risk management as conducted using the ISO31000:2009 risk management model. It aims to analyze the content of the court ruling, and categorize its findings to provide lessons learned for security and safety risk management of aid organizations.

This thesis analyzes details of the Oslo District Court ruling of gross negligence, and applies the findings into the definition and theory-base of security and safety risk management. It is

indeed easy to argue that the humanitarian industry is not the same after the ruling. All organizations realized that their duty of care and security risk management practices must be up to par with the challenging conditions faced in the vulnerable operational environments. The exceptional nature of their work and their working environment does not relieve them of their legal duty of care towards their staff members – on the contrary, it places special demands on the management of these operations.

Based on this, the following research questions will be addressed in the thesis:

- **In the findings of the court ruling, and analyzed based on the definitions of ISO31000:2009 process of risk management, how was the security risk management of NRC lacking at the time of the incident?**
- **How can the findings assist organizations in developing better practices for security risk management in high-risk contexts?**

The research will be explored through a case study of the court ruling. The case is of immense interest to anyone working in not only international development and aid, but also in for-profit enterprises that operate in high-risk environments. The main lesson learned from the incident is that the Norwegian interpretation of the legal duty of care extends equally to all organizations and enterprises regardless of their area of business. If they operate in high-risk areas, security management and mitigation must be scaled upwards considerably to reflect that reality (Oslo District Court, 2015, 14).

While the case was tried in a Norwegian court according to Norwegian common law, the principles and lessons learned are highly transferable. Most European, EU and ETA countries share similarities in occupational health and safety law and the codified duty of care requirements, and where no precedent for previous court cases exists in one's home jurisdiction, courts can look at other countries with similar legislation for reference. It is, however, important to note that the European and Western understanding and application of occupational health, safety and security legislation is not universal. Many legislations do not register similar rights for workers and staff members to seek justice for negligence. Thus, the findings of this thesis are limited to a context where the organization is registered in a Norwegian (Western) legal system and the staff members have a right to file a claim in the Norwegian or similar courts. When an organization in a different jurisdiction judges their exposure to litigation, the different environment of legal risks should always be considered.

The material used for research will be, in addition to the original public court rulings and documents, the significant commentaries, news items, third party analyses and publications. General concepts and theories of security and safety risk management are explored through

leading articles and books in the field. Statistics are referred from the leading organizations specializing in collecting data on INGO operations, safety and security.

This thesis focuses initially on defining the core concepts around humanitarian work, the humanitarian context and humanitarian security risk management. A clear risk management perspective is taken, and it is assumed that the standards of duty of care (legal or otherwise) derive directly as an output of security risk management. Security risk management is introduced by providing a concise overview of the definitions of safety and security from the perspective of management and managerial processes. These core definitions are expanded to provide an understanding of the theoretical and practice-based framework of ISO31000:2009. This framework and its terminology is later examined thoroughly against the findings of the Oslo District Court ruling of gross negligence. The thesis will conclude by providing a sheet of lessons learned and best practices that can be used by all organizations operating in high-risk environments. These lessons learned will be tied to the ISO31000:2009 risk management process.

To highlight, this thesis does not aim to tie the lessons learned to the specific context of the court case tried over the incident in Kenya. Instead, it looks at how high-risk environments in general should be approached in terms of security risk management. The focus is on *transferable lessons learned*. This applies not only to different mission destinations, but also to different organizations, regardless of whether they are for- or non-profit, who have business in high-risk areas. While the case will be studied from the perspective of humanitarian organizations, the approach angle to security risk management in high-risk operational environments will remain transferable.

The approach of this thesis is to look at the standards of security risk management according to the precedent set by the court case and the findings of the court. Duty of care is explored and understood as an output of effective security risk management. It is important, however, to underline that the employer's duty of care is not limited to the legal minimum standards. A strong system of staff safety and security should, in my opinion, be a combination of legal pressure and ethical sense of responsibility to do business reliably and staff well-being firmly in mind.

The decision to use ISO31000:2009 model was made due to my organization Crisis Management Imitative using it as the model for security and safety risk management. While I acknowledge the existence of other models for risk management, the practical purpose of this thesis limits the scope to the one used by the contracting organization.

2.1 Significance of the research question and the industry application

The idea for this research came from my professional background and current occupation in humanitarian security and safety risk management.

Our industry has a dire need for a comprehensive analysis of the rationale and the lessons learned from the NRC case. Safety and security risk management is, based on my observations, often overlooked in many humanitarian INGOs. The focus tends to be on the bare minimum of security management, while overlooking the substantial risk of litigation that might follow an incident.

A lost case in court will often result in enormous financial loss and loss of reputation. Reputation is especially difficult, because earning it back might take a long time or not happen at all. Recovery is made more difficult by the possible loss of funding and partner relations. Aid organizations rely on trust as their main lifeline. Trust between donors, partners and their staff members remains crucial – while the trust between the organization and their aid recipients remains paramount. If these are challenged, operations can rarely continue as needed. To improve and manage security risk, a detailed look, such as this thesis, is needed to understand how negligence happens and how security management can be scaled up to meet the requirements set by the authorities. This is also a useful starter for a discussion on the basic requirements of security and safety risk management, and how to balance them with the reality of not wanting to jeopardize aid recipient trust and acceptance.

I personally and firmly believe that all value creation for an organization starts from first taking care of their staff members and providing them with a safe and secure working environment.

This thesis will be produced to enhance the security and safety risk management standards of the Finnish peacebuilding and conflict resolution NGO Crisis Management Initiative, where the author works as a Security Advisor. The findings will be summarized in a lessons-learned table that will be used as a reference tool for the organization's leadership and other interested parties when making decision on the best practices of security and safety risk management in high-risk operational environments.

This thesis will tackle the complex topic of the court ruling with the aim to provide industry-wide best-practices for the *risk management structures and practices* for all organizations operating in challenging conditions. It will complement the previous study on the topic by focusing on risk management *in general* instead of the technicalities of security management *in particular*. With this study conducted, and previous studies considered, organizations will

be able to benefit from a broad knowledge base for improving their own practices. This is assumed to profoundly benefit the industry.

3 Context and the concepts around humanitarian aid

3.1 Development, humanitarianism, aid work and non-governmental organizations

Humanitarian aid organization, or non-governmental organizations (NGOs), promote development and undertake development projects globally and in different sectors of society.

InterAction defines international development as “the well-being of the world’s poorest and most vulnerable people without compromising the ability of future generations to meet their needs.” (InterAction, 2017). This definition notes NGOs as working to support vulnerable populations suffering from either man-made or natural disasters. The modern approach to development is to approach social problem solving from the perspective of sustainability. This is also highlighted in the definition provided by InterAction.

Governments also engage directly in international development, but often the main actor is an NGO that is being funded by a government body. NGO is defined by the Oxford dictionary “an organization that operates independently of any government, typically one whose purpose is to address a social or political issue.” (Oxford Dictionary, 2017). Collectively, NGOs are often referred to as the “third sector” or the “civil society”.

Social and political issues that NGOs tackle can range from the delivery food rations and medical assistance to supporting third world governments in building sustainable models of governance. Humanitarian principles are closely linked with the goals and definitions of international development. Oxford dictionary defines humanitarianism as “concerned with or seeking to promote human welfare” (Oxford Dictionary, 2017). Thus, humanitarian aid often refers to delivering material aid to vulnerable people in an attempt to promote their welfare. It is important to note that humanitarian aid is often not strictly material, but can also be consultancy to a local authority in how to build models of welfare locally. Indeed, modern perspectives of development are often based on the idea of building capacities in target destinations for sustained development and the ability to remove the reliance on external aid (European Parliament, 2017).

Well-known Finnish NGOs include, for example, Finn Church Aid (Kirkon Ulkomaanapu) who bring food, rations and other aid to vulnerable destinations and Crisis Management Initiative who specialize in supporting peace through informal dialogue and mediation.

International development is a vast field with many different players involved. All organizations have their own models of implementation and logistics. These also differ based on donor requirements and the requirements of their aid recipients. This affects their

standing in the country and the level of security and safety considerations that they need to take.

4 Security and safety risk management

To understand risk management, and how to analyse the NRC case from the perspective of security and safety risk management, it is important to begin by defining the core concepts of security, safety and security management. These basic definitions will feed into a broad understanding of how security risk management acts as a part of a broader risk management framework. Furthermore, understanding the basic concepts will allow the reader to gain a more informed understanding of the lessons learned based on the case study to follow.

Security professionals often look at safety and security through the lens of security risk management. This chapter will unpack the different definitions and provide an outline for security risk management that will be referred to when analysing the case study and its implications for organizations. Different organizations, humanitarian or otherwise, will have developed their own unique ways of approaching security and safety risk management. It is, however, important to note that the underlying principles, definitions and processes remain very similar. The idea of "managing security" has a relatively standardized direction of approach, and this also extends to the attempt to standardize the different definitions around the core concepts within the discipline.

We will begin by defining *risk, security and safety*. The three most fundamental terms that we will be dealing with throughout the thesis. After these definitions, we will put them into the context of *security and safety risk management*. How does a security management system look like – especially in terms of humanitarian operations? This system will then be put into the context of *security risk management*. We will look at how security and safety risk management will support organizations in maintaining the required level of duty of care from the perspective of effective risk management based on the theoretical framework of ISO31000:2009 risk management.

4.1 Risk, security and safety

To study risk, security and safety, it is worthwhile to begin with the definition of **Risk.** This definition can be used as a starting point to broaden the understanding in terms of how risk thinking is applied to manage issues related to security and safety.

Risk has an intuitive meaning of something that can bring us harm or damage us. It is worthwhile to begin by exploring the colloquial definition of risk. Indeed, the Oxford English Dictionary defines risk as "a situation involving exposure to danger" (Oxford Dictionary, 2017). On many occasions, risk is used to imply a negative effect brought about by an adverse

situation. This definition is a good starting point, but does not satisfy the needs of a security risk manager.

Risk can be understood as being broader than what the colloquial definition suggests. Risks can also result in positive outcomes. The case of gambling is a classic example. Betting on cards exposes the gambler to the risk of losing their money, but, with little luck and skill, the gambler might find the cards to be on his side and win more than he initially put at stake. It is clear then that risk should not only signify a negative outcome. Risk researcher Paul Hopkin dissects the definition by giving it three dimensions: that of a *negative* outcome, a *positive outcome* and the risk related to the *uncertainty* of the outcome (Hopkin, 2010, 11).

This thesis will approach the definition of risk from the International Organization of Standardization's (ISO) perspective, as it is a common framework for managing risk. They have defined risk as the "effect of uncertainty on objects" (ISO Guide 73:2009, 2009, 1.1). This definition maintains the idea of risk as a positive, negative or uncertain event. According to Hopkin, most organizations are already relying on this definition, or a definition that closely resembles the one of ISO (Hopkin, 2010, 12). Institute of Risk Management, for example, defines risk as the "combination of the probability of an event and its consequence, including positive and/or negative consequence" (Hopkin, 2010, 12).

For the topic of this thesis, the most important part of defining risk is in understanding its relation to the strategic decision making of an organization. In terms of humanitarian operations, and indeed all non- or for-profit ventures, the balancing of either taking the risk or not is a crucial part of strategic decision-making. For humanitarian organizations, the risk of going in to, for example, Yemen to support the famine-gripped population might be high in terms of their security and safety, but the *positive impact* of helping the population and attracting positive donor and media attention might be high enough to allow for the leadership of the organization to decide on implementing the dangerous project. If the risk is accepted, it becomes the responsibility of the organization to manage the *negative impact* of the uncertainty in a way that adheres to, for the very least, the legal requirements of the organization's home country and translates into tangible solutions of organizational and staff safety and security.

The fundamental failure of NRC to manage the security related aspects of this uncertainty can be seen as being at the core of their incident and the legal proceedings that followed. Furthermore, the same can be said for all organizations facing critical incidents regardless of their area of operations. This is not only limited to environments of **high risk** (or high uncertainty), but indeed all environments where risk is present. Risk scientist Albert R. Wilson has observed that there is no scientific way of absolutely determining that risk does not exist (Wilson, 1991, 98). This means that risk management (discussed in the later chapter) can only

be disregarded at the organization's own peril. An environment is often described as high risk when the number of incidents recorded is found to be high compared to the observed normal. If the risks in an environment are related to war, civil unrest, terrorism or extreme crime, the area is often called a **hostile environment** (BBC myRisks, 2016). A definition of a hostile environment has a clear focus on personal safety and security, but risks are also present when discussing, for example, organization's finances, reputation and strategy (Hopkin, 2010, 150). This thesis will mainly focus on security and safety risk.

Security and **safety** are often the key definitions when looking at risk exposure in humanitarian and other operations of high uncertainty. Like risk, they have an intuitive meaning for everyone, as well as standardized and operationalized definitions for security and safety risk professionals. When thinking about security and safety, it is intuitively clear that a security or a safety incident does not have a positive outcome. Security and safety incidents are **hazard risks** that only result in negative outcomes (Hopkin, 2010, 13). That's why, if an environment is perceived as high risk for safety and security, many organizations are prompted into action.

Both security and safety address the wellbeing of personnel and other assets. Security is often seen as an umbrella term that also includes safety. Merriam-Webster dictionary *defines security* as "the quality or state of being secure, freedom from danger" and *safety* as "the condition of being safe from undergoing or causing hurt, injury or loss" (Merriam-Webster, 2017). These definitions do not yet help a researcher much in finding a clear definition between the two. When studying aviation security and safety, researchers Kenneth Pettersen and Torkel Bjornskau made a distinction that safety deals with *internal hazards* while security is focused on *external threats and attacks* (Pettersen, Bjornskau, 2015, 169). From this, it is possible to derive that safety deals with accidents, incidents and hazardous events without an external attacker. Security, on the other hand, is seen as an incident where an external party commits an attack on the organization or its assets. The difference can be illustrated by taking for example a scenario where a staff member of an organization drives a car during a mission. Difficult road conditions read to the vehicle being crashed against a tree and the driver is injured. This is a safety incident as it was result of involuntary and accidental loss of control of the vehicle on the part of a driver. In another scenario the staff member is being driven by a local driver. For personal reasons, the driver decides to crash the car into a tree to harm the other person in the car. This is a security incident as it is a voluntary attack against the person being transported. Sometimes these incidents overlap, and a safety incident can lead to security incidents and vice-versa. For example, if the car in the first scenario crashes in the middle of the countryside in South Sudan, it leaves the driver exposed to third parties who might be inclined to, for example, rob or kidnap her. This thesis will use this distinction when discussing safety and security.

Security and safety risk can be derived by the combined definition of the previously discussed definitions. As previously noted, Institute of risk management defined risk as the outcome of an event when it is considered from the perspective of its consequences and likelihood (Hopkin, 2010, 12). Thus, to look at safety risk, an organization must take a specific security incident, such as a car crash, and evaluate its likelihood and its consequences. If both are high, it is a **high safety risk event.**

Security and safety risk is discussed in companies and organizations within the concept of **corporate or organizational security.** This definition relates to the question of "whose security?" or "whose safety?". In security analysis, the object that is being secured is called the referent object (Buzan, Waever, De Wilde; 1998, 35). The object is something that is existentially threatened and has a legitimate claim for survival (Buzan, Waever, De Wilde; 1998, 36). In the context of corporate or organizational security, the referent object is the organization itself. This means that the security measures taken are to ensure the continuity of the organization and its operations. In practice, this means that organizations must adopt ways to manage security and safety risk. Staff can often be seen as the key asset of an organization; thus, the protection of staff can be understood as a crucial element of supporting the contingency of the business.

4.2 Security and safety risk management

According to management scientist Fredmund Malik, **management** is defined as the transformation of resources into utility or value (Malik, 2017). **Security and safety risk management** is usually an organization's internal support function. It turns organizations resources (for example security allocated budget, knowledge and human resources) into tangible tools (utility and value) to control the effects of security and safety related uncertainty. These tools vary from individual risk to risk and might include, for example, training, secure transportation, arms or personal security details and medical assistance.

Security and safety risk management falls into the bigger picture of risk management, where modern enterprises and organizations use varied tools of risk management to deal and to react to uncertainty caused by many different factors (Hopkin, 2010, i). Indeed, security risk management should be seen as a small part of the bigger picture of managing all risks related to organizational strategy, value creation and contingency. Other areas of risk management include, for example financial and operational risk management (Hopkin, 2010, 150). For the purpose of this thesis, the focus will be on management of security and safety risk.

European Inter-Agency Security Form is an independent organization that supports humanitarian organizations in security and safety risk management. They define security risk management as a "framework of policies, protocols, plans, mechanisms and responsibilities that support the reduction of security risks to staff". (EISF, 2017, 6). This is a useful

definition, as it highlights that security management is a multi-dimensional whole that spans from the organizational policymaking all the way to field implementation, planning and operational protocol. Ideally, security management is present in every stage of organizational activity. With the supervision of the organizational leadership, it aims to tackle and minimize risks involved on every step of the organization's value creation process.

5 ISO 31000:2009 as a security and safety risk management process

5.1 The process of ISO3100:2009

Economist David A. Garvin defines **organizational processes** as "collections of tasks and activities that together — and only together — transform inputs into outputs." (Garvin, 1998, 1). Security and safety risk management is a collection of many tasks and activities that work together to support the desired end goal of controlling the effects of security and safety related uncertainty. These activities include for example, threat assessments, risk assessments, risk analyses, risk treatment, auditing, training and more. Different organizations have different approaches to establishing their systems of security risk management. Organization might start to manage security risk by, for example, by naming a security manager, conducting a threat assessment, implementing a security risk management programme and working with other departments in implementing security and safety controls. The process of security risk management will vary according to, for example, the size, strategy, resources and values of the organization. For example, an IT company will most likely have a different security department from a humanitarian NGO.

For the purposes of this thesis, we will be looking at the International Organization for Standardization (ISO) defined models for risk management. Their standardized models are widely used, and are often used in the context of not only security and safety risk management, but also risk management in the widest sense of the definition. Many organizations prefer to internally use standardized models of risk management to be able to compare the results effectively. There are also many incentives to promote standardized practices across whole industries. This will promote, among other things, better information-sharing, industry development and public oversight. ISO models for risk management have been created to promote this harmonization. The ISO standardized process of risk management is at the core of what the security and safety department of an organization usually does. By understanding the process, it is possible to understand how security and safety risk is handled from the risk management point of view.

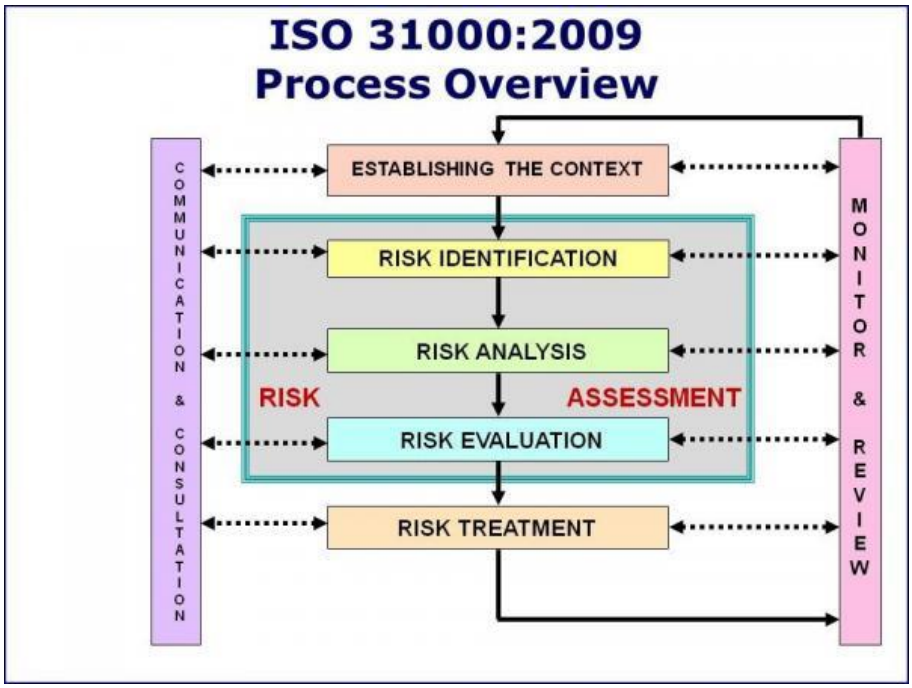


Figure 1, ISO31000:2009 (University of Queensland, 2018)

The chart above is referenced from University of Queensland's staff guide that is intended to demonstrate to their staff how the risk management process works for their organization. It is a standard model for risk management that is used almost universally by all organizations that conduct risk management according to the ISO standards.

It is important to note that the ISO standardized risk management process is intended to be cyclical. It is a model of constant design, implementation, monitoring and reviewing of the risk management results (ISO, 2019). This cycle is sometimes referred to as the PDCA or plan-do-check-act -cycle. This is especially important in high-risk environments where the context is changing rapidly.

This overview will go through all the steps of the risk management process. They will be used as the basis for the research on the case study of the NRC court case.

5.2 Establishing the risk management context

ISO 31000 risk management process starts with establishing the context for risk management. This means that the risk management team will decide on which part of the organizational activity the risk management will target. For a humanitarian organization, the context might be, for example, a rations warehouse in Juba, South Sudan. The team will research the context, decide on the scope of the assessment, consider what internal and external actors are present within the given context and the process, establish communication lines and harmonize assumptions and terminology (International Organization for Standardization,

2009). The establishment of the context can be seen as “setting of the rules” for the process. Determining, for example, the knowledge base used in the process relates to the question of which human resources to utilize (internally or externally) in the risk management steps that follow.

The Department of Finance of the Australian government uses ISO 3100:2009 principles in supporting the development of risk management practices across the spectrum of their public organizations. These practices are also shared across the Commonwealth governments (Government of Australia, 1). They rely on the methodology of establishing the context from the perspective of **the external context, the internal context** and the **risk management context.** This example is used, because it relies of a long tradition of the government (and the Commonwealth governments in general) having implemented ISO 31000:2009. Their approach is also, according to my opinion, very close to the ideal standards set by ISO.

- The external context includes, for example, the following factors: political, cultural, environmental, legal, regulatory, environmental and key trends in the industry (Government of Australia, 2). The failure to research these properly, or identify key personnel that have intimate knowledge in these areas, can result in lacking results in the next steps of the risk management process.

- The internal context relates to the organizational goals, strategy, capabilities of the organization and the organizational culture (Government of Australia, 2). It is crucial to identify the perceived added value and the resources that will be allocated to the process. As risks might also be internal in nature, these factors must be included and noted when risks are managed.

- The risk management context means that all relevant staff members within the organization are identified and included in the process of risk management. Inclusion might include, for example, deciding on who makes decision based on the results of the assessment and how the process itself is managed and implemented into practice (Government of Australia, 2).

The failure of an organization to establish a sustainable context in terms on analysis and resources will lead to lacking results and during the rest of the risk management process.

5.3 Risk assessment

Risk assessment will include the identification, analysis and evaluation of risks in the previously established context.

Identification means that the risk management team will attempt, using a selection of identification tools and resources, compile an as comprehensive a list of risks as possible

related to the context. For the case of Juba warehouse, the risks can range from fire, flood and structural collapse to robbery, terrorism and more. Identification phase can be conducted using, for example, brainstorming, statistical analysis, workshops, interviews, benchmarking and many other tools. In the identification phase, risks are recorded, and their outcomes are described as thoroughly as possible (International Organization for Standardization, 2009). It is important to note that the findings of risk identification rely heavily on the resources (HR or otherwise) allocated to the process during the establishment of the risk management process. If the key individuals with most knowledge on the context are not included, the list of identified risks will remain lacking.

Risk analysis means that the risks are assigned a numerical value based on their likelihood and consequence. This ties the process together with the theory of risk discussed in the previous chapter. Often in security and safety risk management, risk events only have a negative consequence, but it is important to note that many risks are also evaluated by rating their consequence from negative to neutral and positive (International Organization for Standardization, 2009). The likelihood can be determined, for example, based on statistics, expert opinion or other sources. Negative impact (which is often the case with security and safety related hazards) can be determined by, for example, the amount of monetary or productivity loss caused by the event.

Risk evaluation is the final step in the risk assessment. It is used to evaluate, according to the previous findings, as to in which order the previously identified and analysed risks are to be treated. Organizations usually have set up their risk thresholds (how much risk they are willing to accept), and if the findings of the risk assessment show that the context presents individual risks that are above their risk threshold, they will have to be treated. If they cannot be affected (due to the nature of the risk or the lack of organization's resources), it is the decision of the organization's leadership as whether to decide to move ahead with the activity or pull back (International Organization for Standardization, 2009). As risk is the result of RISK = LIKELIHOOD *X* IMPACT, it is easy to evaluate risks hierarchically if the risk analysis process has been done carefully. The list of highest risks should exist, and the evaluation process can act as a review of the findings.

5.4 Risk treatment

Risk treatment is the collective term for actions taken to address the results of the risk assessment. They range from pulling back from the activity altogether to implementing risk specific security policies and practices to counter the uncertainty that is identified in the operational environment. Generally, the likelihood or an impact of an individual risk can be adjusted by implementing strict controls. For example, the perimeter and guarding of the Juba warehouse can be increased. This can reduce the risk of, for example, robbery and terrorism. Humanitarian organizations often rely on acceptance, as the ethical considerations

of increasing, for example, armed protection can adversely influence their reputation in the eyes of the local aid recipients or the local government.

5.5 Communications, review and risk management support

As previously discussed, the ISO risk management model relies on the cycling model. This is evident in the **communication & consultation and monitoring & review** steps that happens throughout the formal process and after it. The implementation and efficiency of the risk treatment measures is evaluated constantly, and when the environment changes the formal process of risk assessment is initiated again. Communication happens during every step of the risk management process. This relates to internal as well as external communications.

5.6 Relation between security management and security risk management

It is important to note that **security management** and security risk management can be used, according to my purposes, interchangeably. I believe that anything that goes under the umbrella of security management is linked to the core activity of context analysis, risk assessment, risk treatment and review. All security management activities derive their goals and purpose from the risk management process. Strictly speaking, security management includes activities that are not part of the risk management process *per se* such as key asset identification, vulnerability assessment, organizational policy craft, internal communications, emergency preparedness and business continuity planning. These activities, however, rely heavily on the risk management processes, and are often risk treatment methods in themselves. The focus of this thesis will be on security risk management, and suggestions on how to derive better value from the process by recognizing the minimum outputs for risk treatment according to the legal duty of care requirements in the context of the case study.

The validity and the care put into security and safety risk management is one of the most important aspects of conducting meaningful security management. If the process is hurried or biased, the results will not reflect the reality of the situation on the ground. This can lead to misinformed decision-making and critical incidents that have far reaching consequences. Single incidents can undermine the reputation and the contingency of an organization – even detrimentally so. The failure of the Norwegian Refugee Council, according to the court, to make realistic decisions based on their staff safety and security caused them to suffer the consequences of poor security risk management.

6 Duty of care, negligence and compliance

The case study and the findings of this thesis discuss the relationship between the employer's **legal duty of care** and security risk management.

Legal duty of care is the organization's responsibility to act with "reasonable care" when dealing with others (Rottenstein Law, 2018). It relates to tort and contract law, and means

that if an organization has acted **negligently** towards a, for example, a staff member, it is liable for the harm caused to that staff member. Duty of care is not codified as such in all legislations, but it is related and highly interchangeable with, for example, the Finnish occupational health and safety legislation or *työtyurvallisuuslaki*. Many legislations retain the idea that it is the duty of the employer to make sure that all reasonable measures are taken to protect staff in the workplace. For example, if a manufacturing plant fails to install emergency stop buttons in their production lines, or if a staff member is not clearly trained on how to use the buttons, in the event of an incident, the employer will be legally and financially responsible of the damages to that staff member.

Depending on the magnitude of the failure to uphold duty of care, an organization may be charged with negligence or **gross negligence.** Gross negligence implies a conscious and voluntary disregard of the need to use reasonable care, which is likely to cause foreseeable grave injury or harm to persons, property, or both (Farlex, 2018). In the case of non-gross negligence, the failure to exercise reasonable care can be involuntary or accidental. Gross negligence implies to either a conscious decision of breaching the duty of care, or a major failure to live up to the expectations of the safety standards in an involuntary way (i.e. a doctor forgetting a foreign instrument inside a patient's body during surgery) (Farlex, 2018).

Finnish legislation discusses the duty of care with a Finnish translation of *työnantajan yleinen huolehtimisvelvollisuus* (Työturvallisuuslaki, 2002, 8§) The law states that the organizations are required to take all necessary precautions to protect the health, safety and security of their employees in the workplace (Työturvallisuuslaki, 2002, 8§). Furthermore, it states that the employer must, according to the nature of the work, do a reasonably systematic assessment of dangers related to the work (Työturvallisuuslaki, 2002. 10§). Appropriate measures must be taken to reduce obvious risk of violence in the workplace, if an obvious risk of violence is present (Työturvallisuuslaki, 2002, 27§).

While legislations differ, many legal systems retain these similar qualities and requirements for the employer. The reasonable and justifiable care is usually the main building block of a law related to occupational health and safety. The language is often quite similar.

For humanitarian organizations, these laws present uncertainties. For example, most legislations discuss health, safety and security *in the workplace*. This is obviously geared towards a broad range of organizations and businesses where the definition of a workplace is self-evident (i.e. a grocery store or a manufacturing compound). Does the definition extend to foreign missions outside the country? If an aid organization, or indeed any organization, sends a staff member to a foreign destination for a week, will that place be considered the workplace? The answer is not immediately clear, and, until the NRC court case, had not been tested in court.

The other problem relates to the definitions of *necessary, appropriate and justifiable measures taken* to protect staff. In environments of high uncertainty, such as a war zone or a fragile state, how do the organizations determine and identify the requirements of necessary, appropriate and justifiable measures taken. How does the court determine these, and how do the organizations know if they have exposure to litigation? NRC ruling has shed light on this as well, and it will be discussed at length in the case study. Identifying these measures is indeed the domain of responsible security risk management. Proper risk management can thus be the critical component of ensuring **compliance** with the legislation.

6.1 Scope of the analysis for duty of care

This thesis is not an analysis of the intricacies of any specific legal system. It will not be a case study on the Norwegian law, and on how it was applied to the NRC case within its legal context. It is also not a reflection on how the Finnish law might interpret the case from the perspective of their legislation.

Instead, the thesis will focus on the broad justifications made by the court on the definitions of necessary and appropriate duty of care. These definitions will be translated into the language of security risk management, and the theory-based model of ISO31000:2009 in particular. The language of employer's legal duty of care overlaps enough across legislations to be interesting in terms of analysis. The failure to meet the necessary, appropriate and justifiable measures is often a failure of security risk management. The incident happened in a high-risk foreign operations context, and the chain of events leading to the incident provides valuable lessons learned for all organizations wanting to ensure legal duty of care and promote effective security risk management, regardless of the jurisdiction in which they are registered.

Thus, this will not be a study on legal duty of care *per se,* but the gross negligence of the ruling is a direct impact of the failure to implement legal duty of care. In many Western organizations. the upper management often has a clear perspective of security risk management as a way to prevent exposure to legal action due to lacking mechanisms of duty of care. The idea of compliance with legal duty of care, according to the aims of this research, is implied to come as a direct result of effective security risk management. Thus, when the idea of duty of care is discussed, it can be understood ***as a direct output of security risk management***.

7 Research strategy and methodology

The following research is qualitative and descriptive case study. It attempts to analyse the contents of the court ruling from the perspective of security risk management with the methodology of theory-based content analysis. Research strategy is the combination of

methodological tools used for the research, while the individual tools are the methods of research (Hirsjärvi, Remes ja Sajavaara, 2009, 132).

Qualitative research is, by nature, holistic and exploratory acquisition of information (Hirsjärvi et.al, 2009, 164). The approach of this study is to look at the court case, and describe and interpret the case from the perspective of the ISO31000:2009 based security risk management framework of definitions. It attempts to find plausible explanations as to how, based on the court's ruling, the risk management of the organization could have been conducted with more efficiency to prevent the incident from happening. Qualitative research is described as finding theoretically plausible explanations on an event or a phenomenon (Tuomi ja Sarajärvi 2009, 85).

Case study can be argued to not be a research method in itself, but a collection of different approaches and data sources to a case that provides added value and interest to a researcher (Swanborn, 2010, 12). Case study object, as is in this case, can be chosen because of the unique nature of the event and its interest as a "watershed" in the given context (Eskola & Suoranta 2005, 65.). In this research, the case is the NRC vs. Dennis court case tried in the Oslo District Court in 2012, and the object of research is the official document of Oslo District Court ruling. It's status as the first major liability and negligence case tried against an aid organization sets it as a unique case to consider for lessons learned.

The research is conducted as a theory-based content analysis. With a deductive approach, an earlier set of established theoretical definitions is applied to the case study object in an interpretive way to understand if lessons can be learned from the findings from the perspective of ISO31000:2009 based security risk management.

Depending on the researcher's goals, content analysis can be both a research strategy and a method. It allows for a structured inquiry into many different forms of communication (written, verbal etc.). As it has a target of inquiry, it is empirical in nature (Tuomi & Sarajärvi 2009, 91). The empirical object of this inquiry is the official document of the Oslo District Court Ruling.

Theory-based content analysis is a deductive approach of looking at the object of inquiry. It takes the framework of definitions as a "given", and attempts to test that framework against the empirical findings of the content analysis. In other words, it attempts to find new meaning on the content studied, based on a defined framework of theory and definitions. (Tuomi & Sarajärvi 2009, 96-98). The theoretical framework of established definitions is the ISO 31000:2009 risk management process and its steps. It relies on the definitions and theory laid out in the previous chapters.

The ruling of the Oslo District Court will be analysed by considering related meanings within the written ruling and the definitions framework of ISO3100:2009 risk management process. The research will compare the ruling to ISO3100:2009 through a set of keywords that bridge the language of the ruling and the language of risk management. Keywords will be assigned into different categories based on the steps in the risk management process. The findings will be presented hierarchically. It is important to note that the study will not attempt to criticize the ruling, but instead takes it as a given. The category that receives most attention in the court ruling is presumed to have had the most weight in determining the court's decision of gross negligence. These categories will be given most weight when analysis and lessons learned are presented in the final chapter.

This methodology will attempt to answer the research questions presented earlier: *"In the findings of the court ruling, and analyzed based on the definitions of ISO31000:2009 process of risk management, how was the security risk management of NRC lacking at the time of the incident?"* and *"How can the findings assist aid organizations in developing better practices for security risk management in high-risk contexts?"*

The complete research process and strategy is as follows:

Phase 1: Choosing the case study object of interest: *Oslo District Court Ruling of NRC gross negligence*.	The case study was chosen because of its nature as a unique and trend-setting event in the humanitarian industry.
Phase 2: Defining the applicable research methodology and definitions framework for the case study: *theory based content analysis*	Theory based content analysis will allow the researcher to find meaning in content that has not been explicitly stated in the object of research. It will allow the exploration of ISO 3100:2009 based security risk management (framework) meanings and similarities in the court ruling.
Phase 3: Categorizing the content according to the theoretical and definition-based framework: *each step of the risk management process is an individual category of interest*	The content is categorized according to every step of the ISO3100:2009. Every step of the process is its own category in the theory-based content analysis. Meanings in the document will be explored according to the following categories:

	• *Establishing the risk management context* • *Risk assessment* • *Risk treatment*
Phase 4: Identifying the keywords and synonyms for every category of inquiry and researching the NRC ruling.	Each category will be assigned, based on the theoretical framework, a number of related keywords and synonyms that reflect similar meanings as the risk management step in question. For each category, The NRC ruling will be systematically scanned to identify how many times these keywords appear.
Phase 5: Presenting findings	Findings will be presented statistically by creating a hierarchy of the observed similarities. If, for example, the number of risk assessment related similarities is highest, it can be presumed that the biggest neglect by the NRC was conducted in that step.
Phase 6: Analysis and lessons learned	Lessons learned will be my reflections based on the findings of the research. They will suggest ways forward for industry professional attempting to develop their own practices for security risk management in high-risk contexts. The result will be a list of suggestions to ensure duty of care in high-risk contexts.

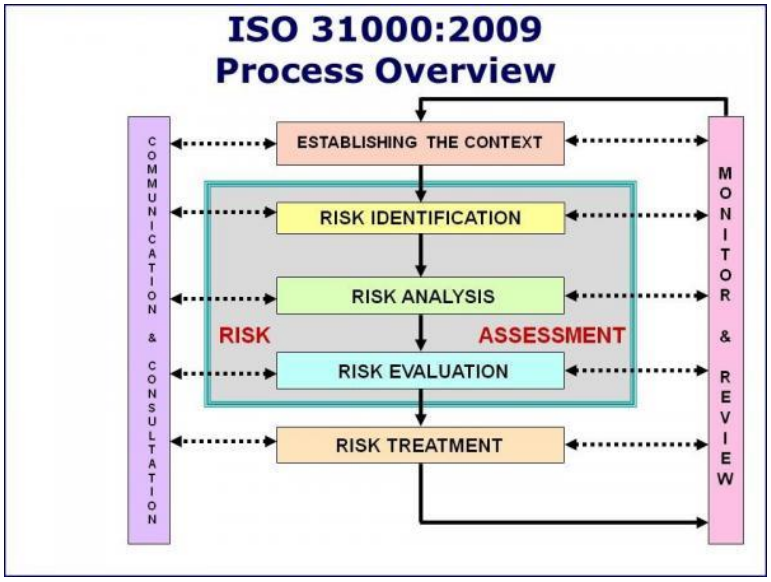
7.1 Establishing the keywords for the research

Keywords will be established based on the similar meanings of the words vis a vie the colloquial discourse (as in the NRC court ruling) and the professional risk management terminology. Colloquial discourse, in this case, means that security is discussed by people who are not security management professionals (the court) and/or do not attempt to describe the event with the terminology risk management. It is important to understand that the NRC

document does not address the level of security risk management in the organization, and is not a direct critique to the risk management methods used by the organization. From this perspective, the relation to security risk management is only implied and is derived from comparing colloquial discourse to the definitions within the process of ISO31000:2009. As an example, the court might say *that the security measure of not using an armoured transport has contributed significantly to the event of the kidnapping having taken place*. This does not mention risk management, but "security measures" mentioned relate directly to the risk treatment step of ISO31000:2009 risk management. The study will attempt to, through a comprehensive list of keywording, attempt to find these kinds of similarities between the court ruling and the process of ISO31000:2009.

It is also important to note that the context within which the keyword is used is analysed to ensure its relevance to the research question. If "security measure(s)" is used as a keyword, it will only be noted if it is mentioned in a context that has contributed to the court's ruling. If it is used by, for example, the court describing its own work process or is mentioned in the table of contents, it is omitted from the findings. If a selected keyword is relevant in only a proportionally small number of its total appearance in the text, its inclusion in the findings is justified with further description.

At this point, it is useful to refer to the earlier graph of the ISO31000:2009 risk management process. The three categories for analysing the court ruling are: *establishing the context, risk assessment* and *risk treatment*.



(University of Queensland, 2016)

It must be noted that the underlying support functions of the ISO31000:2009 that are related to monitoring, review and communications are omitted from this study. This is a rational decision to tighten the focus and narrow the scope of the thesis. They might be referred to

during the findings, but only when relevant to the three main steps of establishing the context, risk assessment and risk treatment. Furthermore, *the questions on establishing lines of communication, monitoring, decision-making and review are intentionally placed in the first category.*

All the categories with the selected keywords are listed below. Keywords are listed as individual words or phrases that reflect, in colloquial language, the professional definitions of the ISO31000:2009 risk management process. For example, the risk assessment includes, in the official terminology, the analysis of the *likelihood* and *impact* of the risk. In colloquial terms, these might be referred to as, for example, *the possibility* and the *outcome* of the risk. All the keywords are established in similar manner to bridge the differences between colloquial and professional language. Furthermore, if a specific concept, such as decision-making or inclusion of relevant staff, is important for a given step of ISO31000:2009, derivatives of these are also included as keywords in the respective categories of the theory-based content analysis. As these phrases can be used in the text in sections not relevant to the inquiry of the study, their relevance and conditions to be used in the findings are specified below.

For the transparency of the study, it is important to highlight that the list of keywords was compiled in two phases. *Prospective* phase included establishing a part of the keywords prior to analysing the object of the research based on the key concepts of ISO31000:2009 and the most common assumed colloquial synonyms. *Retrospective* phase included a brief analysis of the court ruling and finding the terminology used in its language to complement the list of keywords established prospectively. The combined findings of these two phases resulted in the following keywords for each category:

- **Category 1: Court ruling from the perspective of establishing the risk management context**

  The keywords will emphasize the action points relevant to the establishment of the risk management context. They include the following words and their derivatives:

  - *Context, security situation, political situation, security environment* – relevant if the court case discusses the context of the case when describing NRC's failure to understand it properly.
  - *information, knowledge, aware(ness), understand* – relevant if the court mentions it in the context of the organization having had too little information of the context.

- *Relevant people/personnel/staff, include, inclusion* – relevant if the court mentions the lack of relevant staff members included in the safety/security related processes.

- *decision/decision making* – relevant if the court addresses the lack of established lines of decision making in the case of security related issues

- **Category 2: Court ruling from the perspective of risk assessment**

Risk assessment framework looks at how the court ruling has implied that the steps of risk identification, analysis and evaluation had been lacking. It will look at lessons learned to enhance these steps to avoid the mistakes made by the NRC in their risk assessment processes.

- *Identify, identification, predict* – Relevant in the context of the court discussing the NRC's failure to identify or predict risks to an adequate level

- *Risk, Likelihood, probability, possibility* – Relevant in the context of the court discussing the NRC's failure to analyse the likelihood of a risk to an adequate level.

- *Impact, effect, outcome* – Relevant in the context of the court discussing the NRC's failure in predicting the impact of the risk to an adequate level.

- *Analysis, analyse, evaluate* – Relevant in the context of the court discussing the NRC's failure in analysing and evaluating their risks properly.

- **Category 3: Court ruling from the perspective of risk treatment**

Risk treatment is the most practical part of the inquiry, as it relies heavily on how the reasonable and justifiable treatment measures should have been implemented in the actions of NRC. This section makes references to the previous categories as needed, but attempts to arrive to over-arching findings in providing reasonable and justifiable risk treatment methods based on the general concept of high risk operational environments in the humanitarian context.

- *Treatment, control(s), measure(s)* – Relevant in the context of evaluating how different controls and measures were applied in treating security-related risks

- *Mitigate, mitigation* – Relevant in the context of discussing how different mitigation measures were taken to reduce security related risks.

- *Action(s) (taken), implement (controls)* – Relevant in the context of actions taken or implemented to prevent risks.

- *Minimize, prevent, reduce* – Relevant in the context of actions taken to minimize and reduce risk.

These categories will be analysed from the perspective of the theoretical foundations and definitions laid down in the previous chapters. The study will look closely at the court findings and attempt to place them in the categories based on the steps of the risk assessment process. The analysis will rely on the theoretical framework of ISO31000:2009 principles and guidelines from the perspective of security and safety risk management, but will be my and for the use supporting the learning of the industry that I work for. The validity of the researcher's findings will be left on the reader to judge. The findings will attempt to broaden the concepts of each of these steps, but will not introduce any new definitions or core theories that have not been presented during the chapters on core definitions.

8 Findings and analysis of the theory-based content analysis

This chapter lays out the findings and the analysis around the theory-based content analysis. It is structured in a way that first presents the findings of the study objectively, and then provides a subchapter of analysis on how the mistakes can be avoided in the future for organizations operating in similar environments.

Findings are denoted as the number of references found for each category and each keyword category. The number of references reflects the exact number of times the keyword appeared in the text. As the Oslo District Court ruling of the Dennis vs. NRC case reflects the reasoning and the thinking of the court that led to the ruling of gross negligence, it is assumed in the methodology of the study that *the more time certain issues are referred to, the more they carried weight in the court's decision.* For example, if the court refers multiple times to the lack of certain security controls, these are listed as being references in the third category for risk treatment.

Findings are laid out by first comparing the *overall findings* between the total number of references for each category. This is used to draw a big picture of the references and analyse which step of the risk management structure of ISO31000:2009 can be interpreted as having had most failures in, and thus had most weight in the ruling. After the overall findings, all the three categories are analysed individually and in depth. The attempt is to draw conclusions as to how risk management according to ISO31000:2009 can be used to avoid the faults made by the NRC at the time of the incident.

8.1 Overall findings: ISO31000:2009

These overall findings attempt to draw case-specific conclusions on how the findings differed between categories, and if any assumptions can be made on how they differed.

The overall findings are:

- **Category 1: Court ruling from the perspective of establishing the risk management context:** *Total 49 references*
- **Category 2: Court ruling from the perspective of risk assessment:** *Total 117 references*
- **Category 3: Court ruling from the perspective of risk treatment**: *Total* 104 references

From the big picture perspective, it can be analysed that a connection can be seen with all categories. Almost equal weight was given to categories 2 and 3, with the first category not far behind. It can be assumed, that in this case, the failures in risk treatment are directly linked to failures in the risk assessment phase. Furthermore, the failures in all categories can be traced to the inadequate establishment of the risk management context in the first step. This can be seen as the major overall finding of the study. It is, according to my analysis and the findings, very difficult to identify any individual step of the risk management process that was at the forefront when the ruling on gross negligence was made. Instead, failures during every step of the risk management process led to the combined effect of creating an environment where the incident could take place and happened without adequate risk mitigation measures in place.

The court underlined on many occasions that the overall requirement for NRC to justifiably understand the risks in the location (category 2), and establish reasonable mitigation measures around those risks (category 3) were crucial in deciding on if they had acted in negligence. In the ruling, the findings were often presented together, and they underline the key finding of the analysis that there is a direct link between the failure to assess risk properly and the failure to treat them properly.

"In making this assessment (of gross negligence), the Court has in particular attached importance to the existence of specific information that it was probable that a kidnapping could take place and that in the worst case, this could have a fatal outcome. Several practicable and effective alternative courses of action existed. Despite this, reasonable and necessary security measures were not implemented. Quite the contrary; the changes to the security plan made the risk of kidnapping increase substantially. Staff were not notified reasonably in advance of changes to the security measures, and as a consequence thereof

they were exposed to increased risk. Consequently, the decision-makers acted with gross negligence both when establishing the security measures and in that staff members were not informed of their role and the increased risk to which they were exposed. (Oslo District Court, 34)"

This excerpt from the ruling can be interpreted that mistakes were made during every step of the risk management process. This also reflects the overall findings of the study where implicit references to most of the steps in the risk management process could be found in the ruling. Overall, it can be said that the gross negligence did not happen during any individual step from the perspective of the ISO31000:2009 risk management model. Instead, mistakes were made from the beginning, and the failures in each step fed into failures in the next. Thus, a more careful look at the different mistakes made during every step is crucial in informing well-rounded understanding of the failures that led to the incident and the ruling of gross negligence after the fact.

According to my analysis, the following lessons learned can be drawn from these failures:

- **All the risk management steps feed into the success of the following steps. It is therefore crucial to not overlook the importance of, for example, the establishment of the risk management context in the light of wanting the risk management program to succeed.**

- **All levels of the organization must be included in the risk management process to avoid gaps in information and decision-making.**

8.2 Category 1 finding: ISO31000:2009: Establishing the Risk Management Context

The findings in the Category 1 were divided between the different keywords in the following manner:

Context	8 references
Security/ political situation, security environment	15 references
Information, knowledge, awareness, understand(ing)	12 references

Include, Inclusion, relevant people/personnel/staff	5 references
Decision, decision-making	9 references

Context-related keywords were applied by the court when analysing NRC's general preparedness in operating in the Dabaab Refugee Camp area. The difficulties of working in the area had been highlighted by multiple different internal and external studies. The court had taken these into account when analysing the level of context-specific preparedness of the NRC. The excerpts to follow from the court ruling highlight the primary trends of the failures in establishing the risk management context. They are iterated throughout the content analysis in different forms, but share the common thread of the major failures within the section of the process:

"As a consequence of these (security) circumstances, the security situation in Dadaab deteriorated strongly. The UN raised the risk level in Dadaab from level 3 to level 4. In September 2011, a Kenyan driver from the organisation CARE was kidnapped, and in October 2011 two foreign women from Doctors Without Borders (MSF) were kidnapped. (Oslo District Court, 3)"

Furthermore,

"The NRC's handling of staff security had been very weak for *some time, both in terms of understanding the security context and in terms of implementing applicable minimum standards. (Oslo District Court, 8)"*

This example highlights the overall theme of the ruling, where the different sections of the risk management process can be seen feeding into each other. "understanding the security context" and "implementing applicable minimum standards" reflect all steps of the risk management process. The failures can be seen to stem from the lack of basic context awareness. One of the court's most vocal rulings can be linked to the failure in context analysis:

"Based on the evidence, the Court is of the opinion that there should have been a stronger security thinking and understanding in the Dadaab area. (Oslo District Court, 21)"

Furthermore,

"In the opinion of the Court, this indicates that the NRC's decision-makers should have acted differently, and they should at least have sought advice from competent security advisors

before making the decision. (Oslo District Court, 20)" – This refers to the decision of not using armed escort during the mission to the refugee camp.

These sections highlight the fundamental failures in establishing the risk management context. As referred to earlier, context establishment relies on finding the right people to involve in the later steps of risk assessment and treatment. When choosing this team, it is the responsibility of the manager to ensure that enough people are involved as to provide the most context awareness possible. Well-informed process of risk identification requires the engagement of staff that provide the highest level of context awareness possible.

Overall, it can be said that NRC failed to establish the right teams and risk management structures. Decisions were made without proper consultation. Furthermore, while most Security Advisers are not formal decisionmakers in their organizations, neglecting their advice can reinforce negligence in cases of critical incidents. This is highlighted in:

"The decision-makers with regard to the security plan had, in the view of the Court, themselves the responsibility for securing a satisfactory basis for decision-making, including securing advice from advisors with security competence. (Oslo district Court, 30)"

It can be said, based on the court's findings and the ruling, that decisions made related to the risk management practices were made without clear input from the field staff and internal advisory elements that had most knowledge of the risks involved in that context. This failure to establish clear structures of informed decision-making led to the failure to predict risks and the overall ruling of gross negligence after the fact.

According to my analysis, the following lessons learned can be drawn from these failures:

- **When establishing the risk management team, it is crucial to include staff/personnel with intimate knowledge of the local security context and the developments in the region in question.**
- **These personnel must be included from the beginning and have a clearly defined role in all the steps of the risk management process.**
- **Clear decision-making structures must be established from the beginning. If changes in controls or treatment are made, they must be made with clear procedures of consulting the relevant advisory elements.**

8.3 Category 2 findings: ISO31000:2009: Risk Assessment

Failures in Risk assessment was given most attention in the court ruling. It is, according to ISO31000:2009, the longest section of the process as it comprises of risk identification, risk

analysis and risk evaluation. This might contribute to it including the most references in the findings. It can be said, however, that the failures of NRC were done on all levels of the risk assessment process, and contributed greatly to the incident and the ruling of gross negligence after the incident.

Identify, identification, predict	3 references
Risk, likelihood, probability, possibility, impact, effect, outcome	115 references
Analysis, Analyse, Evaluate	2 references

The overall failures of NRC in the risk assessment happened through a repeatedly mentioned trend of failing to evaluate the risk of kidnapping adequately, and the failure to balance the likelihood of that risk with the risk of IEDs and other risks in the area. Overall, the findings of the court stress that the kidnap risk was externally accepted to be elevated. This referred to, not only certain internal advisories in NRC, but the findings of other NGOs and organizations operating in the region. The broad consensus was that armed escort should be used to minimize the risk of kidnap.

"There had been several kidnapping incidents and the risk of kidnapping was as high. (Oslo District Court, 7)"

Norwegian Refugee Council failed to emphasize the likelihood of kidnap risk in their own risk assessment, which led to the failure of choosing the proper mitigation measures later in the process. Furthermore, the following finding was made by the court to further emphasize the criticality of not overlooking the kidnap risk in the region:

"Because of the security situation, no VIP visits were performed after the kidnappings in the autumn of 2011. According to the witness Daniel Hardy from the Danish Refugee Council (DRC), no other NGOs carried out any VIP visits at the time. He explained that they had performed VIP visits prior to the kidnappings of employees of CARE and Doctors Without Borders, but that all visits were halted after that. He explained that they experienced an escalation of the security situation and that the risk of kidnapping was considered to be increasing and unacceptable. (Oslo District Court, 14)"

Overlooking the broad trends in the risk analyses of other organizations, NRC had decided to carry on with the VIP visit. This reflects either negligence on part of the decision-makers, or the failure to realistically identify, analyse and evaluate kidnap related risks in the region. The NRC had, according to the court findings, attempted to balance the risk of kidnap with their own assessment of high risk of IEDs. This finding overlaps with the third category, but their rationale is relevant to the second category as well.

"There was also a risk of being hit by an improvised bomb or road bomb, a so-called IED (improvised explosive device), but it is not a given that the risk of such attacks would increase noticeably in the case of an armed escort being used. (Oslo District Court, 8)."

The failure to emphasize the right risks during the phase of risk evaluation led to the NRC making the critical mistake of overlooking the risk of kidnapping by prioritizing the risk of IEDs. This was a cumulative failure of context analysis, risk identification and risk analysis. Furthermore, it can be seen in the light of failure to make informed decisions about the security risks facing staff in the region.

Furthermore, the court ruling empathized the lack of information security related risk assessment. They found that the inability to assess and treat information security related risks in relation to the kidnap risk was highly overlooked and contributed not only to the incident, but the overall ruling of gross negligence.

"Furthermore, the NRC has itself acknowledged that there was a failure in the information security risk and that as a consequence the kidnappers may have come to know that a VIP visit was to take place on the day in question. This acknowledgment is supported by other evidence in the case. (Oslo District Court, 22)"

The decision to undertake a VIP visit without an armed escort and the lack of information-security related planning and risk assessment contributed to the incident and the ruling of gross negligence. It also places questions on the gravity of the failure to overemphasize the risk of IEDs in light of all the risk factors pointing to the elevated risk of kidnap (security environment and the information security). Even the highest levels of NRC security risk management did not have the clear picture of information security related findings of the risk assessment:

"He (NRC HQ Security Advisor) explained that if he had known of the breaches of the information security, seen in conjunction with the amended security plan, he would have asked for the visit to be cancelled. (Oslo District Court, 20)"

This poses difficult questions for NRC in terms of the scope of their risk assessment (did it not include information security?) and their decision-making structured as it relates to context

establishment (were the higher-level security personnel not aware of the risks related to information security breaches?).

According to my analysis, the following lessons learned can be drawn from these failures:

- **The risk assessment process must be done with close cooperation of the field personnel who have the most inmate knowledge of the local security environment**
- **Overall trends, the risk assessments and the incident experiences of other organizations operating in the area must be a crucial component during every step of the risk assessment.**
- **Risk assessment must be able to look at broader risk dynamics around the threats and dangers in the area. Namely, the physical security risks must not be overemphasized in cases where, for example, information security risks feed directly into the likelihood of these events materializing.**

8.4 Category 3 findings: ISO31000:2009: Risk Treatment

From the court's perspective, the third category focused on the different security measures and controls, and how the failures in implementing them properly led to the incident. Security measures and controls can be understood as belonging to the category of risk treatment, as they are, according to risk management methodology, tools to reduce either the likelihood or the impact of the risk.

The court worked on finding the causal relationship between different risk treatment methods, and how they lacked the ability to prevent the incident from happening. Furthermore, they analysed if alternative risk treatment methods could have been implemented to change the course of the events.

Treatment, control(s), measure(s)	56 references
Mitigate, mitigation	8 references
Action(s), implement	22 references
Prevent, reduce, minimize	18 references

The findings in the third category are given almost equal weight to the second category. As

mentioned earlier, this highlights the fact that the failures in risk assessment directly feed into the failures in risk treatment.

The overall failure in implementing proper security measures came, according to the court, in three major categories: information security, inclusion of security staff and physical security. According to the court, the combined effect of failures in all of these categories led to the incident taking place and the impact of the risk being amplified to the extent of the staff members getting kidnapped and injured. The combined effect of these failures is articulated by the court in the following manner:

"The concrete errors relate to the failing information security, the fact that the visit was performed with a high profile, that a visit was made to IFO II, that the duration of the visit exceeded the recommended duration, as well as the lacking presence of security staff. Nor should the visit have been performed without the use of an armed escort. (Oslo District Court, 8)"

The lack of armed escort was referred to as a reference of duty of care throughout the court's ruling. This became especially relevant in the context where other organizations had used armed escort as a routine measure for an extended period of time due to alarming developments in the security context. From the perspective of security management, it is interesting to note that courts clearly used other organizations (whether they'd be similar peer-organizations or organizations of different nature) as a comparison as to what constitutes a standard operating practice in the area:

"The reports show that the use of armed escort became a mandatory part of recommended security measures from the end of October 2011. (Oslo District Court,15)"

And,

"However, it had been an established practice for several months that because of the serious security situation, no other VIP visits had been carried out. Against this backdrop, it was to be expected that the organizers of the visit would contemplate the security situation with utmost seriousness, and at least implement necessary and reasonable security measures when it was decided that the visit was to be carried out. (Oslo District Court, 20)"

With these observations, it can be concluded that the implementation of security controls relies not only on a purely internal assessment of the risks, but also a careful analysis on how other organizations operate in the area. If an incident takes place, considerable attention is being paid to the standard operating procedures (SOPs) of all regional actors. If a deviation from a regional SOPs perspective is observed, as was in the case of Norwegian Refugee

Council, it can present as being the “tipping point” for the courts to rule that gross negligence took place. As the previous citation from the court ruling indicates, the SOP in the region was that VIP visits were not conducted, and the threshold to deploy armed escort was low. In case of NRC, a clear deviation from both current “regional norms” was observed. The courts placed significant attention on the fact that the NRC had failed to deploy armed escort even as they made a clear decision to take the risk of deploying a VIP staff member to the area.

NRC justified the lack of armed escort as being a mitigation measure for minimizing the likelihood of improvised explosive devices (IEDs), which were commonly used by militants in the area. Many witnesses to the court testified this being a justification fabricated after the fact, as the court concluded that any thorough risk management process would have identified that the risk of IEDs is not lowered by the lack of armed escort. In fact, this was testified as being on the contrary:

“A deterrent element shall generally be included in the security measures, and that in reality this indicates that an armed escort should have been used. He (Chris Allan, witness to the court) explained that ordinary movements inside the camps normally would take place without an escort, but that an escort should be used in the case of an international or high profile visit. Chris Allan also emphasized that the use of an armed escort did not increase the risk of IEDs. (Oslo District Court, 19)”

The courts also identified that errors were made in terms of how the security controls were implemented, and how changes in the controls were handled in terms of the decision-making structures of the NRC. This relates equally to the first category of the theory-based content analysis, but has relevance on the implementation of controls as well. NRC had initially planned to use armed escort, but made the change on the last minute to use unarmed escort. The decision-making structure and the process that fed information from the field to the decision-makers was seen as lacking, and was evidenced to have been a root cause of not having the proper security controls in place:

“The report (conducted on the incident by the NRC) contains a list of several weaknesses in the handling of security, and a list of several recommended measures to improve security. She explained in court that there were deviations in the understanding of the security situation and that those responsible had to understand that context analysis is a tool to make it possible to reach good decisions concerning security measures. (Oslo District Court, 20)”

This proves the earlier observation, that the failures in the early stages of the risk management process fed into the failures that led to inadequate application of controls in the

field level. These failures contributed into the disaster that led to the incident and the gross negligence in the NRC case observed in this study.

NRC made the case that their security measures relied on the overall principle of *low profile*. This means that they believed that increasing security measures, going in armed and with a convoy would raise their profile enough as to increase the risk of drawing unwanted attention. This was rationalized as to feeding into the increased likelihood of attacks, assaults, IEDs or kidnap.

The courts observed that the only tangible evidence of implementing low profile related to the removal of the armed escort as a security measure. The courts observed that this did not constitute as a reasonable level of low profile security implementation, as multiple failures were identified in managing information security practices:

"Information security was inadequate, from the outset in late May many staff knew of the proposed visit and increasingly third parties were informed. The choice of date was inappropriate, it called people in on a day that was normally a non-working day and as such incentive staff members were given a week's notice of a VIP visit. (Oslo District Court, 22)"

And,

"No other measures were implemented for the visit to Dadaab to keep a low profile, apart from the removal of the armed escort. In connection with this, the Court mentions that the security advisors who gave evidence in the case stated that the removal of the escort was not an adequate measure for averting neither the risk of kidnapping nor IEDs. (Oslo District Court, 25)"

These accounts of the court amplified the fact that in order to successfully implement low profile risk mitigation, the focus should be in how information is shared and how the knowledge of the event is controlled. The court found multiple situations where the inhabitants of the camp were informed of the upcoming visit. Furthermore, no provable vetting was made as to who was trusted with the information and who was not. This fed into the court's conclusion that low-profile security management was not adequately implemented and would could not justifiably be used as an argument as to why the deviations of the region-wide SOPs were made.

According to my analysis, the following lessons-learned can be drawn from these failures:

- **The failure to implement proper security controls and risk treatment methods is directly linked to the strength of the context analysis, peer-organization analysis and the involvement of all levels of organizational decision-makers and advisors within the organization.**

- **The decision to change risk treatment methods must be done with all available resources (human and other). If, for any reasons, these resources cannot be utilized at the time, the change should not be implemented to preserve accountability.**

- **Courts place considerable weight on how other organizations operate in the region. To avoid exposure to negligence, all controls and SOPs should be up to comparative standards. If deviations are made, they should be made with absolute discretion and with proper due diligence.**

- **Low profile approach is not criticised as such in the case of NRC. If implemented, it requires a careful examination of what constitutes a low-profile approach. This relates to proper implementation of information security measures that minimize the risk of critical mission information leaking into wrong hands.**

9 Chart for lessons learned and for organizations to improve ISO31000:2006 -based security risk management practices in high-risk contexts

The following boxes highlight the overarching lessons learned for organizations that want to enhance their risk management practices in light of the gross negligence ruling for the Norwegian refugee council. All lessons learned are placed in the distinct categories in relation to the ISO31000:2009 process:

ESTABLISHING THE CONTEXT

- Include personnel from all levels of the organization and from the field in the risk management team
- Establish clear lines of communication between team members
- Identify decision-makers and train them in their role
- Brief and raise awareness of the risk management process across all staff working within the context of the process

RISK IDENTIFICATION

- Include the staff working in the field in the risk identification process
- Always use peer-organization analysis as a tool for risk identification
- Always conduct thorough context analysis
- Use external intelligence as much as possible, do not rely on in-house intelligence alone
- Include all levels of organization in risk identification. This creates ownership and also feeds into process-related risk awareness
- Be cautious as to not over emphasize certain categories of risks over others. Include experts of information security, communications and others as well as the more traditional physical security experts.
- Have a legal professional support risk identification from the perspective of external compliance risk and exposure

RISK ANALYSIS

- When analysing risks, do not overlook how failures in processes and communications can lead to further risks and other undesired outcomes
- Include the core risk management team in risk analysis
- Use peer-organization support and lessons learned in defining and brainstorming possible outcomes

RISK EVALUATION

- Evaluate the relevant risks not only from the perspective of physical security -related incidents, but also from the perspective of how process-failures can lead to unforeseen consequences. Do not overlook risks that are directly not related to critical incidents.

RISK TREATMENT

- Do not overlook regional SOPs and best practices and operational “norms”.
- Do not overlook risk treatment methods that relate to informing, training and sharing of responsibilities
- Understand your overall strategy for security management (e.g low profile) and identify the key treatment methods that promote that very strategy.
- Do not hesitate to revisit the previous stages of the process if new information or new risks arise during the planning process of risk treatment.
- Establish clear plans on how/when/why to deviate from the original risk treatment plan.

10 Conclusions and further research

To conclude, it is useful to refer to the original research questions and analyse if the findings answered all the questions posed.

10.1 Conclusions for the first research question

The first research question was: *"In the findings of the court ruling, and analyzed based on the definitions of ISO31000:2009 process of risk management, how was the security risk management of NRC lacking at the time of the incident?"*

The study referred to the court ruling as the single document that summarized the findings and the rationale of the court. It was examined through a theory-based content analysis that relied on the established terminology of the ISO31000:2009 risk management standard. While the court did not mention risk management explicitly, it has many implicit references to similar processes and steps within the established risk management framework. Theory-based content analysis was found, according to my opinion, a useful tool of extracting this implicit information from the court text.

One of the main findings of the research was that, in the Dennis vs. NRC court case, implicit references to risk management failures were found throughout the entire process. Keyword-findings were spread surprisingly evenly distributed across all the different steps of the ISO31000:2009 process. The assessment was made that the case demonstrates that equal importance must be given to every step of the risk management process. Failures in the earlier steps of the risk management process had fed into failures later. This created an environment where inadequate safeguards were in place, and the incident could happen and cause serious harm to staff members in question.

Establishing the risk management context must be done in collaboration with the field team and the headquarters. Norwegian Refugee Council had failed to engage all relevant staff members in the organization. This resulted in the failure to establish the level of context awareness and knowledge required in the risk management team to tackle the complex operational environment. Furthermore, clear lines of communication and decision-making were not established from the beginning. In ISO31000:2009 -based risk management, these are a fundamental part of establishing the risk management and risk response team during the phase of establishing the context for the risk management target.

Lacking expertise in the risk management team led to inadequate risk assessment. Risks were either ignored, as was the case with information security related risks, or, as was the case with IED risk, analyzed improperly. The risk of IEDs was seen as higher than the risk of kidnap, which led to the failure to prioritize security controls that could have either prevented or reduced the impact of the incident.

NRC had chosen to take a low-profile approach with security management. This led to risk treatment methods that were inadequate. The catastrophic failure to implement proper risk treatment methods was a direct result of inadequate risk analysis. NRC had evaluated the risk of IEDs to be higher than the risk of kidnap, and decided to not use armed escort. This would, according to NRC's analysis, lead to a lower profile presence and reduce the risk of militant attacks with IEDs. According to the court's findings, the decision to not use armed escort did not only contribute to the impact of the kidnap, but did not reduce the risk of IEDs. Furthermore, no information security precautions were made to keep the mission secret. Risk treatment methods must be directly and clearly in line with the risk assessment. The low-profile approach for security management was made with inadequate backing from the findings of the risk assessment.

Multiple references were found in the court ruling to the effect of implicitly referring to failures in the NRC risk management practices. Overall, it can be concluded that NRC failed during every step of their risk management process to produce meaningful security. The failure started from the first steps of establishing the context, and resulted in the failure to implement effective security controls.

The study was conducted by using the ISO31000:2009 related synonyms and colloquial definitions in attempting to find implicit references to risk management practices in the court ruling. The validity of the study relies on the validity of how the different categories and keywords were established. This provides opportunities for future researchers to set the framework of the study in a different way to find more intricacies in the content and its implicit refences and meanings. Furthermore, it would be beneficial to explore more in-depth how a single distinct step in the risk management process influenced the court's decision. This can refer to, for example, a more detailed look on risk management process support functions such as communications. This was mentioned on numerous occasions in m study, but did not receive a full study of its own. This was a rational decision on my part to limit the scope of the study on the three main steps of the risk management model.

Furthermore, future studies on the topic might also benefit from bringing more specific information on the topic into light. The study conducted here can be criticized for pointing out something that can be seen as self-evident. As pointing out something that my security professionals take for granted: that all steps of the risk management process matter equally. This was reflected in the findings where it was not able to point out any single step of the risk management process in particular that the NRC had failed in. While, in my opinion, it is valuable to find confirmation to this broad effect as well, the industry can benefit tremendously from a more targeted study that has a narrower scope and more narrow perspective. This would allow a more detailed consider how one distinct element of security management in particular can have tremendous impact on the entire process.

10.2 Conclusions for the second research question and the industry application

The second research question was: "*How can the findings assist organizations in developing better practices for security risk management in high-risk contexts?*"

All the findings from the first section of the study were summarized in a single sheet of lessons-learned and best practices drawn. These findings can assist organizations in developing their own practices for operating in high-risk environments. This is especially beneficial, in my opinion, for humanitarian organizations that routinely work in challenging contexts and often rely on low profile approaches in their security management and risk treatment methodologies.

They key findings for *establishing the risk management context* include the participation of correct staff and the engagement of correct human resources for the risk management team. The leading manager must understand, on a broad level, the basic demands of the field and be sure to include all relevant personnel in the process of risk management from the beginning. Clear lines of decision-making and communication need to be established from the beginning. It is crucial to understand that failures in establishing the risk management context will feed into inadequate risk management outputs later in the process.

Risk assessment must be done with utilizing thorough analysis of how all organizations operate in the region. The importance of external intelligence is crucial. Internal and external stakeholders on all levels of the organization must be involved, and departments dealing with information management and HR, for example, must not be overlooked. Careful work must be done to evaluate the risks in order to understand how emphasizing certain individual risks and approaches to risk mitigation will create requirements to adequately understand the residual risks of the decisions. In the case of the NRC, the decision to implement a low-profile approach was not complemented with adequate information security precautions. A holistic approach to risk assessment is crucial for the success of the risk management program and the risk treatment in general.

Effective *risk treatment* is determined by a grounded reliance on the practices and findings established in the previous steps of the risk management process. In order to avoid negligence in cases of incidents, it is important to not overlook how organizations in general operate in the area. SOPs should be thought in terms of regional and local operational norms. If a deviation from the common SOPs is made, it must be justified on the grounds of a thoroughly conducted risk assessment.

In my opinion, the lessons-learned are useful and thorough. They provide a sound base for organizations to make decisions over how security should be handled in the contexts where they work. The process of extracting lessons learned from the theory-based content analysis

was seamless, and in my opinion, the research method deployed was extremely useful for this kind of research that aims to draw practical conclusions from a case or a selection of research material.

The industry application of the findings will provide a thorough breakdown of how the lessons learned can be taken into consideration during every step of the ISO31000:2009 risk management process. These findings are beneficial in providing a thorough picture of how organizations should enhance their risk management practices to reduce the occurrence of similar incidents in the future. When combined with the previous studies on the topic, a broad overview of lessons learned is beginning to be established for the industry.

The overall findings must be understood in being a result of a very particular study on a very particular event of interest. It is, therefore, necessary for all organizations to use their own discretion and context awareness in making security and safety related decisions. The findings can be criticized as to being too particular given the context and the target of the study. However, a rational decision was made to attempt to broaden the scope of the findings to fit as naturally as possible to the context of diverse environment of organizations working in many different countries.

It is possible, as future research, to compile a similar table of findings to reflect only the NRC case the lessons learned for that organization. While the findings would be more specific and limited in terms of universal applicability, they would benefit from the possibility of a more in-depth look of how similar situations could be handled better. Furthermore, these more detailed findings could be translated to a broader base to provide even a better sense of how one organizations operate, and indeed, as the court ruling proved, for other organizations to understand how to do better peer-organization benchmarking and harmonization of controls and SOPs. The lack of NRC's ability to do this well enough was one of the contributing factors in their gross negligence. This, of course, applies to organizations other that NRC as well. As a point of reflection and analysis, every organization can benefit from a direct and limited look into how a particular organization failed or succeeded in risk management.

Overall, the findings and answers to both research questions serve the aim of providing more information to organizations that are serious about minimizing incidents and providing adequate levels of duty care to their staff members. Humanitarian organizations are no different from other organizations in their need to protect their staff and create a safe and secure working environment.

References

Printed sources and publications:

Buzan, Barry; Waever, Ole & de Wilde, Jaap. 1998. Security: A New Framework for Analysis. Lynne Rienner Publishers.

Development initiatives. 2017. Global humanitarian assistance report 2017. Development Initiatives.

EISF. 2016. Duty of Care: A review of the Dennis v Norwegian Refugee Council ruling and its implications.

EISF. 2017. Security Risk Management: a basic guide to smaller NGOs. European Inter-Agency Security Forum.

Eskola, Jari, & Suoranta, Juha. 1998. Johdatus laadulliseen tutkimukseen. 7. painos. Tampere: Vastapaino.

Garvin, David A. The Processes of Organization and Management. 1998. MIT Sloan Management Review, 1-12.

Government of Australia, Department of Finance. 2016. An Overview of Risk Management Process. Government of Australia.

Hirsjärvi, Sirkka; Remes, Pirkko & Sajavaara, Paula. 2009. Tutki ja kirjoita. Helsinki: Tammi.

Hopkin, P. Fundamentals of Risk Management. 2010. The Institute of Risk Management.

Humanitarian Outcomes. 2016. NGOs and Risk: How international humanitarian actors manage uncertainty. Humanitarian Outcomes.

Humanitarian Outcomes. 2017. Aid Worker Security Report 2017. Humanitarian Outcomes.

Humanitarian Policy Group. 2012. Humanitarian Space: A Review of Trends and Issues. Humanitarian Policy Group.

International Organization for Standardization. 2009. ISO/Guide 73:2009(EN). ISO.

International Organization for Standardization. 2018. ISO 31000:2018. Risk Management – Guidelines. ISO.

Oslo District Court. 2015. Judgment 25.11.2015 – Steven Patrick Harris vs. the Norwegian Refugee Council. Oslo District Court.

Pettersen, K.A., Bjornskau T., 2015. Organizational contradictions between safety and security. Safety Science 71, 167-177.

Swanborn, Peter. 2010. Case Study Research: What, Why and How? SAGE Publications.

Tuomi, Jouni & Sarajärvi, Anneli. 2009. Laadullinen tutkimus ja sisällönanalyysi. 5., uudistettu laitos. Helsinki: Tammi.

Työturvallisuuslaki, 2002. 23.8.2002/738. Suomen laki.

Wilson, Albert R. Environmental Risk: Identification and management. 1991. CRC Press.

Electronic sources

BBC myRisk, 2016
http://www.bbc.co.uk/safety/safetyguides/highrisk/hostile-environment
Accessed 3.12.2017

European Parliament, 2017
http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2017)599411
Accessed 3.12.2017

Farlex, 2018. Gross negligence.
https://legal-dictionary.thefreedictionary.com/gross+negligence
Accessed 7.1.2018

Hoppe, Kesley; Williamson, Christine. 2016. Dennis vs Norwegian Refugee Council: implications for duty of care. Humanitarian Practice Network.
https://odihpn.org/blog/dennis-vs-norwegian-refugee-council-implications-for-duty-of-care/
Accessed 11.1.2018

Humanitarian Practice Network. 2010. A Closer Look at Acceptance.
https://odihpn.org/magazine/a-closer-look-at-acceptance/
Accessed 11.1.2018

InterAction, 2017
https://www.interaction.org/work/development
Accessed 3.12.2017

International Organization for Standardization, 2009. ISO 31000:2009. Risk Management – Principles and Guidelines.
https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-1:v1:en
Accessed 6.1.2018

International Organization for Standardization, 2018. The new ISO 31000 keeps risk management simple.
https://www.iso.org/news/ref2263.html
Accessed 24.4.2018

IRIN, 2015. NRC kidnap ruling is 'wake-up' call for aid industry.
http://www.irinnews.org/report/102243/nrc-kidnap-ruling-%E2%80%98wake-%E2%80%99-call-aid-industry
Accessed 24.4.2018

Malik, 2017
http://www.malik-management.com/en/malik-approach
Accessed 3.12.2017

Merriam-Webster, 2017. Safety.
https://www.merriam-webster.com/dictionary/safety
Accessed 3.12.2017

Merrian-Webster, 2017. Security.
https://www.merriam-webster.com/dictionary/security
Accessed 3.12.2017

Oxford Dictionary, 2017, NGO
https://en.oxforddictionaries.com/definition/ngo
Accessed 3.12.2017

Oxford Dictionary. 2017. Risk.
https://en.oxforddictionaries.com/definition/risk
Accessed 3.12.2017

Oxford Dictionary, 2017. Humanitarian.
https://en.oxforddictionaries.com/definition/humanitarian
Accessed 3.12.2017

Rottenstein Law, 2018. Duty of Care.
http://www.rotlaw.com/legal-library/what-is-a-duty-of-care/
Accessed 6.1.2018

The Guardian, 2015. Steve Dennis and the court case that sent waves through the aid industry.
https://www.theguardian.com/global-development-professionals-network/2015/dec/05/steve-dennis-court-case-waves-aid-industry
Accessed 24.4.2018

University of Queensland. 2015. Enterprise Risk Management – Procedures.
https://ppl.app.uq.edu.au/content/enterprise-risk-management-procedures
Accessed 6.1.2018

Figures